

REMARKS

Claims 49-87 remain in this application, with Claims 1-48 previously cancelled, and Claims 49, 58, 66, 70 and 80 amended. Applicants respectfully request review and reconsideration of the application in view of the foregoing amendments and following remarks.

As discussed previously, the present invention is directed to a novel approach for allowing a client to maintain state with a web application operating on a remote server while protecting the user's security and privacy. According to an embodiment of the invention, the client generates a unique state variable at its end (referred to as a "state identifier"), and then communicates the state variable to the server for use in associating different web page requests as part of the same user session. This has great benefit, since web browser applications no longer need to be "open" in the sense that web servers no longer need to store information on the client machines to maintain state with the client. The client may selectively transmit the state variable to the server as an http header with each uniform resource locator ("URL") request. The server receiving these requests compares the state variable to information stored in a database to determine if the user has a current transaction status that should be taken into account in the server's response. Applicants have amended the claims to clarify that the method and system for maintaining state between a client and a server occurs "without the server transmitting to or storing on the client any state-related information."

The Examiner rejected Claim 80 under 35 U.S.C. § 102(b) as anticipated by Dustan et al. The Examiner also rejected Claims 49-52, 56-61, 65, 66, 68-72 and 76-87 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al. and further in view of Denning. Applicants respectfully traverse these rejections.

Dustan et al. discloses a method for accessing information that is consistent with the above description of the prior art. In particular, a client accesses a network server by requesting a logon menu. A logon input is then communicated to the network server, which in turn communicates the logon input to a database server. The database server verifies the logon input and generates a unique session identification number, which is

communicated to the client for storage on the client computer. In subsequent communications with the server, the client provides the session identification number, enabling the server to verify that the session identification number and logon input are valid.

The Examiner refers to the communication by the client of the account number and password as providing the "state identifier" described in the patent application (citing to Dustan et al., Fig. 5, reference number 176). The account number and password are validated to determine whether to permit client access to the network. See col. 17, Ins. 58-67. But, it should be appreciated that the account number and password are not used by the server to maintain state, *i.e.*, to determine whether a particular communication is part of a common user session. Instead, the server generates a session ID for the purpose of maintaining state and sends that information back to the client. See Fig. 5, reference numbers 212, 216.

On this point, the Examiner asserts that Applicants' argument is not persuasive and contends that Applicants do not describe the role of the account number in full. Applicants respectfully disagree. The Examiner quotes text from Dustan et al. that clarify that the session ID alone is used for maintaining state--the account number is not used for this purpose. The Examiner argues that Dustan et al.'s use of the account number is consistent with "Applicant's interpretation of 'state' as disclosed in the Specification." Respectfully, the Examiner is ignoring the clear text of the claims that recite "comparing the subsequently transmitted state identifier with the initially transmitted state identifier stored in the database, and if there is a match, then associating said second communication with said record of the first user session." This limitation is not suggested or disclosed by Dustan et al.

Hence, Dustan et al. discloses the conventional use of cookies that are generated at the server end and communicated to the client for storage on the client. This conventional state-identifying method causes the significant security concerns discussed above, and that are overcome through the use of the present invention. Dustan et al. fails to suggest or disclose a system in which a session ID (or other state

variable) is generated by the client and communicated to the server to maintain state ***without the server transmitting to or storing on the client any state-related information.***

The Examiner acknowledges that Dustan et al. does not disclose the use of location information in the generation of an identifier, and proposes the combination with MacDoran et al. and Denning. MacDoran et al. discloses a method for authenticating the identity of a remote user through the use of information specific to the location of the user. Likewise, the Examiner cites Denning as supporting motivation to combine Dustan et al. with MacDoran in view of its disclosure of "authentication through geodetic location." This teaching is of little applicability to the present invention to the extent that the invention is directed to maintaining state between client and server, and not to authentication of the client. Neither MacDoran et al. nor Denning disclose any use of location information as a state variable, and hence fails to make up for the deficiency of Dustan et al. For each of the above reasons, the foregoing grounds of rejection should be withdrawn.

The Examiner further rejected Claims 53-55, 62-64, and 73-75 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al., and further in view of Fraker et al. Fraker discloses an apparatus for logging position and time-at-position data in accordance with time and position data broadcast by a number of earth orbiting satellites. The Examiner cites Fraker merely for its disclosure of temporal data. Fraker otherwise fails to suggest or disclose anything relating to maintaining state between client and server, and specifically fails to suggest or disclose the desirability of using temporal data in a state variable. There is no teaching or suggestion for the proposed combination. This ground of rejection should be withdrawn.

The Examiner further rejected Claim 67 under 35 U.S.C. § 103(a) as unpatentable over Dustan et al. in view of MacDoran et al., and further in view of Hunter. Hunter discloses a JAVA function that causes cookies to expire when the browser exits (see public void Cookie.setMaxAge). Notably, this attribute is defined by the creator of the cookie, *i.e.*, the server, and hence the client cannot control the

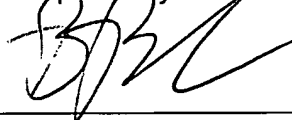
Serial No. 09/880,308
January 17, 2007
Page 13

expiration of the cookie. In the present invention, the client creates and deletes the state identifier, providing direct control over the security of the communications. Hunter fails to suggest or disclose a method for maintaining state between client and server in which the client generates the state identifier and can also delete the state variable upon termination of the browser session. This ground of rejection should also be withdrawn.

In view of the foregoing, the Applicants respectfully submit that Claims 49-87 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

To the extent necessary, Applicants petition the Commissioner for a four-month extension of time, extending to January 18, 2007, the period for response to the Office Action dated March 14, 2006. A check in the amount of \$1,190.00 is enclosed for the four-month extension of time (\$795.00) pursuant to 37 CFR §1.17(a)(4) and for request for continued examination (RCE) (\$395.00) pursuant to 37 CFR § 1.17(e). The Commissioner is authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,



Date: January 17, 2007

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000